# Before The
# Federal Communications Commission
# Washington, DC 20554

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Encryption of Amateur Radio | ) | RM-11699 |
| Communications | ) | |

## Comment of Bruce Perens

## Introduction

### *My Standing To File on This Matter*

1. I hold an Amateur Extra Class operator license, and corresponding station license with call sign K6BP.

2. I am one of the pioneers of digital voice communications over Amateur radio, as founder and evangelist of the Codec2 project (http://Codec2.org/). That project has created an Open Source ultra-low-bandwidth digital voice codec for use on Amateur Radio and elsewhere.

3. More recently, I have been evangelist and manager for the FreeDV project (http://FreeDV.org/), which distributes a free application program that provides clear digital voice communications over HF radio while using half as much bandwidth as an SSB communication.

4. It is likely that some form of the systems that I have helped to create, Codec2 and FreeDV, would be made use of for encrypted voice communications over Amateur Radio, if such are allowed.

### *Introductory Comments*

5. I discuss the matter at hand in detail in this comment, however I'll state my recommendation up front: **This matter has not been discussed**

**sufficiently *within the Radio Amateur community* for rule-making to go forward at this time.** At present, the Amateur community as a whole is insufficiently informed to be able to form a cogent opinion on the issue.

6. Before it is considered, such discussions should be carried out, including articles in major Amateur publications by both supporters and dissenters, and balanced pro-and-con presentations at many major Amateur conferences.

7. **Thus, I recommend that FCC dismiss the petition without further consideration at this time, and without prejudice regarding a future petition. Such a petition could re-open the issue once the Amateur community has been able to debate it and, if desired, construct a national plan or standard for the use of encryption in emergency communications.**

8. The allowance of encryption over Amateur Radio could seriously damage the Amateur service if the rules designed for it do not mitigate the potential for abuse, especially given the insufficient resources allocated to enforcement of Amateur rules.

9. Given the reality of FCC's miniscule budget for Amateur matters, the verification of whether the content of encrypted transmissions is appropriate for the Amateur service must rest mainly on the shoulders of Radio Amateur volunteers.

10. But encryption will prevent monitoring by volunteers unless some provision is made for that, and monitors must be required to maintain the confidentiality of Protected Health Information. Thus, if encryption is to be allowed in the Amateur service, a good design for volunteer-based verification of lawful operation is necessary. And the volunteers must have recourse to FCC for enforcement in the case of inappropriate use of encryption.

11. The petitioner, Mr. Don Rolph, was unaware of the existence of the HSMM-Mesh system (http://hsmm-mesh.org/) and other WiFi-like systems that operate on Amateur frequencies, until informed by me via

telephone and email on June 25, 2013, more than a month after his petition was accepted. Thus, Mr. Rolph did not consider in his petition the greater potential for abuse in those systems, which provide vastly greater bandwidth than the *Winlink* node that Mr. Rolph operates.

## Discussion

### *Framing the Issue*

1. To frame the issue, the matter at hand is whether to allow *private communications* within the Amateur Service and, if so, when and how to allow them.

2. *Private communications* are communications that are not expected to be monitored by or entered into by anyone other than the intended sender and recipients. Unintended recipients are restricted from attempting to monitor these communications through legal or technical means. The technical mean in this case would be encryption.

### *Present Rules*

3. No part of Part 97 presently authorizes private communications. The only permission presently allowing encryption for the purpose of obscuring information, in 97.211(b), is intended to protect *commands to a machine* (a space satellite), not communication with any person.

4. 97.113(4) prohibits messages encoded for the purpose of obscuring their meaning, and the neophyte might take this as a blanket prohibition upon encryption. However, *it does not prohibit encryption for the purpose of authentication*, for example an encrypted password or a digital signature. Such items can be transmitted in encrypted form while the message content remains in the clear.

5. In particular, a digital communication can be carried out in a form that, through digital signature (http://en.wikipedia.org/wiki/Digital_signature), verifies the identity of the operator while the message remains in the clear. Encryption for the

purpose of authentication, presently allowed under Part 97, is sufficient for the purpose of preventing access to Amateur digital networks by non-amateurs. It is not necessary to encrypt the message content.

6. Thus, the proposed change does not introduce useful features to Amateur radio *other than private communications.*

### *The Rationales Offered for Allowance of Private Communications*

7. I list the rationales I'm aware of here, including ones I don't agree with.
8. The petitioner, Don Rolph, offers these justifications for allowance of private communications:

   a) Encryption of certain emergency data is required (e.g. specific patient information covered by HIPAA, identification of sheltered persons, etc.)

   b) Certain emergency information is required for tactical purposes to be encrypted (e.g. certain logistical information: movement of food, medical supplies, certain movements of personnel).

   c) For national security reasons certain emergency communications should be encrypted.

9. Other parties offer these rationales for the allowance of encryption:

   d) The WiFi-like hardware used by HSMM-Mesh (http://hsmm-mesh.org/) operators incorporates Part 15 WiFi hardware internally, and uses the 2.4 GHz WiFi band as an intermediate frequency (IF), transverting that to an Amateur band. Other Amateur networks use the 2.4 GHz WiFi channels as their fundamental frequency, sharing them directly with Part 15 users.

   WiFi users can receive, and can be received by, WiFi-like equipment that uses 2.4 GHz channels as its intermediate frequency. Inter-operation is thus possible between Amateur equipment and Part 15 WiFi equipment operated by unlicensed individuals. And of course this is true for Amateur networks that directly share 2.4 GHz channels with Part 15 users.

Thus, a means to exclude non-Amateurs from these networks is necessary. Some HSMM-Mesh operators propose to use the existing Part 15 WiFi 802.11i Security implementation (http://en.wikipedia.org/wiki/IEEE_802.11i), also known as *WPA2*, which would obscure the meaning of the entire communication.

### *The Proposals Offered For Allowance of Private Communications*

10. I list the proposals I'm aware of here, including ones I don't agree with:

11. Mr. Rolph's petition is to limit encryption to emergency communications and drills, based on present rules in Australia.

12. Some HSMM-Mesh operators have submitted comments in this proceeding proposing the allowance of encryption of their entire communications using the existing 802.11i security mechanism, with the primary purpose of excluding non-Amateurs from their networks.

### *Discussion of HIPAA*

13. *The Health Insurance Portability and Accountability Act of 1996* regulates the use and disclosure of *Protected Health Information* (PHI) through its *Privacy Rule*, which went into effect in 2003. The text of the act is tremendous, at 1200 pages, but the main relevance of the act upon Amateur Radio emergency communications can be easily explained:

14. The providers of health care services: doctors, hospitals, insurance companies, and their staffs; are all subject to the Privacy Rule. They must only disclose Protected Health Information to those who are directly concerned with keeping the patient healthy, and *only* the information that is directly necessary for the patient's care. Protected Health Information is information about a patient's medical status combined with identification of that patient. One purpose of restriction on disclosure of PHI is to protect people from discrimination based on

their medical status. For example, the landlord of an apartment for rent should not be provided with health data that would facilitate discrimination against prospective tenants who are HIV-positive or who have sickle-cell anemia.

15. The consequences for health-services providers who improperly disclose Protected Health Information are fines levied by the Federal Government, and lawsuits on behalf of patients who complain that their information has been disclosed improperly. Fines as large as $1.5 Million dollars have been assessed. A lawsuit will generally cost many Millions of dollars in legal fees to defend, even if the defendant wins the case.

16. Of course Amateur communications can, in the usual case, be monitored by everyone as if they were broadcasts.

17. Thus, hospitals and other health-services providers could conceivably be directed, by overanxious legal counsel or management, to avoid making use of the emergency services of Radio Amateurs for fear that the Amateurs will expose them to multi-Million dollar liability by disclosing Protected Health Information during an emergency.

18. The Amateurs themselves are not, in general, at risk under HIPAA. It is the health-care providers who are subject to HIPAA. In addition, Amateurs may be protected by “Good Samaritan” laws.

19. However, a lawsuit can be brought against any person or organization, and the cost of legal representation leading to the dismissal of a frivolous and invalid suit can still be staggering.

20. It is not appropriate to modify regulations of the Amateur service simply to dispel *fear* of a lawsuit rather than an actual conflict in law. So far, there is no case-law on the issue of Amateur communications and HIPAA, and no reason to believe that there shall be any.

### *The Department of Health and Human Services States That Encryption is Unnecessary*

21. The Federal Government Department of Health and Human Services, charged with enforcing HIPAA, has a FAQ regarding HIPAA at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/incidentalu%26d.pdf that discusses whether encryption of radio services is necessary. They write:

> Q: Does the HIPAA Privacy Rule require hospitals and doctors' offices to be retrofitted, to provide private rooms, and soundproof walls to avoid any possibility that a conversation is overheard?
>
> A: No, the Privacy Rule does not require these types of structural changes be made to facilities.
>
> Covered entities must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information. This standard requires that covered entities make reasonable efforts to prevent uses and disclosures not permitted by the Rule. The Department does not consider facility restructuring to be a requirement under this standard.
>
> For example, the Privacy Rule does not require the following types of structural or systems changes:
>
> * Private rooms.
> * Soundproofing of rooms.
> * **Encryption of wireless or other emergency medical radio communications which can be intercepted by scanners.**
> * Encryption of telephone systems.
>
> Covered entities must implement reasonable safeguards to limit incidental, and avoid prohibited, uses and disclosures. The Privacy Rule does not require that all risk of protected health information disclosure be eliminated.
>
> Covered entities must review their own practices and determine what steps are reasonable to safeguard their patient information.
>
> In determining what is reasonable, covered entities should assess potential risks to patient privacy, as well as consider such issues as the potential effects on patient care, and any administrative or financial burden to be incurred from implementing particular safeguards.

```
Covered entities also may take into consideration the steps that
other prudent health care and health information professionals are
taking to protect patient privacy.
```

### *The Petitioner's Rationale Regarding HIPAA and Privacy of Medical Information is Specious*

22. As explained by the Department of Health and Human Services, encryption of *a medical facility's* radio communications is not necessary for HIPAA compliance, thus implying that encryption also unnecessary for Amateur Radio volunteers that handle medical data in emergency situations. HHS recommends other strategies than encryption in the same document, such as not discussing the information in a manner that can be identified with a particular patient.

23. The typical procedure for avoiding the transmission of Protected Health Information on a radio call would be to identify a patient by an institution's transient internal number for that patient (rather than a publicly identifiable number like a social-security number) or a description. Examples of these would be “admission number 10214” or “A 42 year old man in insulin shock”. Decoupling the identification of the patient from the data on their medical condition removes the information from the category of Protected Health Information, which must be identified with a patient. Encryption is not at all necessary to protect the patient's privacy using this procedure.

24. Encryption will not always be available, especially under the constraints of emergency operation, and emergency communications can not wait until it becomes available. Under Mr. Rolph's rationale, HIPAA issues re-emerge whenever Amateurs transmit Protected Health Information while encryption is unavailable. However, by using proper procedures to decouple the patient's identifying information from their medical situation, the HIPAA issue is always avoided.

25. Even when encryption is available, the security of encryption provided by Radio Amateurs is dubious, due to limitations of the particular encryption mechanisms available to them and, more seriously, defects in their operation of such systems. It is unlikely that

Amateur groups will be reliably able to maintain the physical and electronic security of equipment holding encryption keys, as many commercial and military organizations have failed to do that reliably. This will lead to access to the encrypted messages by unauthorized parties. Much of the equipment available to Amateurs, especially equipment based on Part 15 WiFi, has firmware that is known to have security flaws. In particular, any router that provides “PIN number” access, also known as *WiFi Protected Setup,* can be penetrated in seconds due to an un-repairable flaw in that algorithm (https://krebsonsecurity.com/2011/12/new-tools-bypass-wireless-router-security/). Even when equipment is without flaws, programs such as Aircrack-ng (http://www.aircrack-ng.org) can be used to extract the cryptographic keys from on-air transmissions.

26. Ultimately, it is the responsibility of the health services provider to avoid disclosing Protected Health Information in an identifiable form to Radio Amateur volunteers for further communication. Amateurs are not trained to operate under HIPAA (a 1200-page law) and it is never likely that they will receive more than a fraction of the HIPAA training required of a medical professional.

### ***The Petitioner's Tactical Information Rationale is Specious***

27. Mr. Rolph proposes that encryption is necessary to protect information regarding the movement of food, equipment, and personnel in an emergency situation.

28. This sort of secrecy may be necessary for certain kinds of international assistance where the rule of law is in abeyance, such as to Haiti during their recent earthquake. However, the use of encryption in international Amateur communications would require authorization at the level of ITU first, or through agreements between individual nations. Authorization by FCC could only follow such action.

29. However, it is likely that such authorization will never be necessary, due to the availability of other communications modes for such communications. In particular, the ships and aircraft used to

transport international disaster relief material have their own communications systems outside of the Amateur service, which will necessarily be used for tactical information regarding the actual place and time of a delivery. The security of these systems is far outside of the scope of domestic Amateur regulation.

30. Mr. Rolph's rationale for domestic allowance of encryption is regarding the potential for robbery of food supplies, a food riot resulting from an intercepted communication, or danger to emergency personnel or equipment resulting from an intercepted communication. The need for such secrecy in *domestic* communications that would be handled by Radio Amateurs is the stuff of apocalyptic fiction, and Amateur rules would not be at issue in such a situation.

31. Communications regarding the dispatch of medical personnel should *not* identify the particular individuals involved, whenever possible. This should be sufficient to avoid the situation of a particular person who is being stalked and who might be endangered by an intercepted communication. However, it would take a concatenation of many factors for such a thing to happen: an emergency worker who is being stalked, disaster communications regarding that worker that are handled by hams, information in a message that identifies a particular worker, and a radio-scanning stalker. All of this seems sufficiently unlikely that a rule-change would be inappropriate.

### *The Petitioner's National Security Rationale is Specious*

32. Mr. Rolph speculates that Amateurs might be in a role to transmit *National Security Information* which would be at risk if not encrypted. I boggle at why such information should or would ever be given to Radio Amateurs to handle. Perhaps this is an attempt to make rules for use *after* the fall of civilization.

### *The Petitioner Has Not Demonstrated A Need*

33. Amateur radio is presently useful for disaster communications, as a distributed resource of personnel who can provide improvised

communications systems to meet *emergent* needs, as well as organized and pre-rehearsed communications services to meet *expected* disaster needs. The capability to handle emergent situations through improvisation is a specialty of the Amateur service. It is facilitated by the service's unique incentives for operators to gain technical knowledge and to construct and modify their own equipment. It is a maxim in emergency planning that “you never get the emergency that you've planned for.” It is thus likely that the capability of Amateurs to improvise will remain desirable in any future scenario.

34. The petitioner has *speculated* that encryption may be necessary to continue to make Amateur Radio disaster services palatable to a served medical organization, but he has *not actually demonstrated* that this is so. Our numbers, operating skill, equipment, and our ability to improvise should be sufficient to continue the desirability of Radio Amateurs to served agencies.

## Encryption Could Block Self-Enforcement by Radio Amateurs

35. Amateur Radio depends upon self-enforcement of its regulations. In 2012, FCC disclosed only 47 letters sent to accused violators of Amateur regulations, among 709,500 licensed Amateurs. In contrast, the Bureau of Justice Statistics reports a rate of incarceration of 492 sentenced prisoners per 100,000 of the general U.S. population in 2011 (http://www.bjs.gov/content/pub/pdf/p11.pdf). While this is an “apples and oranges” comparison, it is sufficient to demonstrate that FCC does not allocate more than a tiny pittance of resources toward Amateur enforcement. The first rank of enforcement of Amateur regulations must thus be the Amateurs themselves, and most “enforcement” today happens through social pressure rather than legal citation. On those rare occassions that FCC actually becomes involved, it is almost always after the violations are well-documented by Amateurs as part of their pleading for enforcement.

36. For Amateur self-enforcement to work, Amateur volunteers must be capable of receiving the message so that they can verify that the content is lawful. Encryption places a hurdle in the way of

self-enforcement because it makes reception of the message impossible unless the encryption algorithm and key can be duplicated. When the cryptographic algorithm is known, the computing time required for the recovery of a cryptographic key can be short or it may be greater than a human lifetime. How long it takes depends on the cryptographic algorithm and key size.

37. For the 802.11i WiFi security algorithm, more commonly known as WEP2 for “wired equivalent privacy version 2”, there are a number of encryption algorithms and key lengths available. There are many security breaking programs available, a popular one is Aircrack-ng (http://www.aircrack-ng.org).

38. The key sizes in consumer equipment using 802.11i have been deliberately restricted to make decryption tenable to intelligence agencies and law enforcement, and the security provided is expected to be sufficient for a home network with very short range. When this same equipment is used for an Amateur wide-area network, we get a lose-lose situation: the key is long enough to deter Amateurs who would casually monitor communications for enforcement purposes, but it is short enough to make key-breaking possible for those who are motivated enough to expend the resources necessary to break into a particular network. So, we get a network that is insecure, with a deficit in enforcement.

39. This same lose-lose situation exists with surplus commercial or municipal communications equipment such as DMR (also known as MOTOTRBO), which has recently been subject of another Amateur rule-making: RM-11625. That Motorola system provides encryption which is sufficient to deter casual monitoring for enforcement by Amateur volunteers. However, due to the age of the equipment and the increasing speed of modern computing, the 256-bit key used in DMR/MOTOTRBO can be broken by a determined person willing to put in the time and resources. The recent trend of putting the graphics-card processor to use for decryption has resulted in supercomputer-like decryption capability in conventional desktop computers.

40. It is not impossible that given this enforcement deficit, that links using Amateur frequencies could be used for all sorts of violations in the name of “emergency communications.” A common example might be the use of a WiFi-like link on Amateur frequencies to extend an internet connection between two points, over which would travel all of the usual content of internet users. There is no reason to object to such a link within Part 15 regulations, but Amateur bands are reserved for other purposes.

41. How could we enforce in the presence of encryption? It would take an awkward system, but a possible one. Amateur volunteers like today's “ARRL Official Observers” would have to contract not to disclose Protected Health Information. Users of encryption would have to be required to log the encryption key and other information about the communication, and surrender it to such Observers on request. Under these constraints, it would be possible for Amateur volunteers to verify that encrypted communications are lawful.

## Encryption Creates a Special Class

42. Under the proposed regulations, when an Amateur hears an encrypted communication on Amateur frequencies, they will have to assume that it is an emergency communication. They won't be able to verify its nature on their own without the encryption key. They won't be able to break into the communication to ask the operator what's going on, because encryption locks them out. Their only choice will be to vacate the frequency, for fear of interfering with an emergency communication.

43. Thus, encryption creates a special class of operation that forces other Amateurs to abandon a frequency as soon as they detect its presence. That class has all of the priority of an ongoing emergency communication, without any capability for others to verify that an emergency communication is actually in progress.

## Encryption Internationally

44. Current ITU regulations for Amateur Radio prohibit encrypted Amateur communications between nations. But there isn't a method of stopping encrypted communications at national borders, especially communications using HF frequencies or satellites.

45. For nations to continue to authorize Amateur Radio, they must perceive it as harmless. There is no reason for anyone to expect that an encrypted communication is harmless.

46. DX-peditions are already viewed with suspicion by authorities in many nations. Amateurs who are personally known to me have had encounters with military and police authorities while attempting to operate a DX-pedition station in another nation. If encrypted communications happen on Amateur radio, other nations are likely to view them as espionage. This will tend to have a chilling effect upon DX-peditions.

## Encrypted Amateur Radio and The National Interest

47. The Federal Government has an interest in communications interception for purposes of National Security. Recent news has made *that* abundantly clear. Amateur radio is a direct peer-to-peer communications mode. Unlike the telephone system, it is not mediated by a communications provider that will honor “security intercept” requests as telephone companies do. It has international range in the case of HF and satellite. The need to monitor and police such a system, if encryption becomes common, would engender political pressure domestically against the further allowance of Amateur radio.

### *Encryption Will Work Against Interoperability*

48. Commercial digital communications systems for Amateur Radio have, unfortunately, all been made incompatible with each other, deliberately, by their manufacturers. D-STAR, DMR/MOTOTRBO, and Yaesu's new digital system are all incompatible with each other. The purpose of this is to create system monopolies for a particular

manufacturer, and thus drive sales of that manufacturer's units exclusively within a market.

49. So far, Icom has come out on top of this game with the popular D-STAR system, but this has not deterred Yaesu from creating a brand-new incompatible system. Astonishingly, Yaesu's new system is derived from DMR/MOTOTRBO, but has deliberately been made sufficiently different that it will not interoperate with DMR/MOTOTRBO.

50. Only DMR/MOTOTRBO presently offers encryption, but as other manufacturers pick it up they are sure to implement it incompatibly with their competitors, further reducing interoperability of Amateur equipment.

51. The Codec2 (http://Codec2.org/) and FreeDV (http://FreeDV.org/) projects are attempting to reverse this trend by offering their systems to all manufacturers to integrate as 100% Open Source software, including the digital voice codec – the technically most difficult portion. However, reversing the market trend of incompatibility is difficult enough for these projects *without* the introduction of encryption to the mix.

### *97.211(b) – Encryption and Amateur Satellites*

52. 97.211(b) presently allows encryption that obscures the content of the message for control of Amateur satellites. But only *authentication* is necessary for secure ground control of a space resource. It doesn't matter if the commands are transmitted in the clear, as long as there is a valid digital signature accompanying the command.

53. Why, then, is encryption that obscures the message content authorized for this use? Historically, Amateur satellites have been so simple, technically, that the “encryption” they provided was little more than exclusive-OR of one or two data bytes and a small pre-determined number.

54. High-orbit Amateur satellites have historically had very simple

computers because they have to operate in a high radiation environment. They have been based on the antique 1802 CPU architecture because only that CPU has been available to us in the radiation-resistant silicon-on-sapphire implementation (“SOS”, for short). They have had no ROMs, but downloaded their entire operating program from a ground-station communication using a *hardware-only* downloader before they could be booted. Complicating this situation is the “astronomical” cost of silicon-on-sapphire computing hardware. AMSAT, unable to afford many SOS integrated circuits, has survived on donations of surplus devices from government and commercial satellite companies.

55. Eventually, it will be technically possible for all Amateur satellites to be commanded using digital signature for authentication rather than encryption for the purpose of obscuring the message content. This advance waits upon the availability of the appropriate radiation-resistant computing hardware at a reasonable price. The day will come when historical satellites requiring content encryption are out of service, and all operating units support digital signature. At that time, it will be possible to withdraw 97.211(b) without harm to the Amateur Satellite Service. Given the 40-year operating longevity of some of the higher-orbit Oscar satellites, I can't forecast the date of this event.

## Solving the HSMM-MESH Access Problem

56. We still need to solve the access problem for HSMM-MESH and other operations where unlicensed interlopers using Part 15 equipment can enter the system. However, new regulation is not necessary for this solution. Current regulation allows the use of encryption that does not obscure the message content but does provide authentication of the identity of the originator of a message. Digital signature can be used to provide this authentication. This is probably outside of the scope of the existing 802.11i facilities, and will require special software. Fortunately, the HSMM-MESH group already uses the OpenWRT (http://openwrt.org/) version of Linux as their router operating system. Since their system is Open Source, they can modify it as necessary to provide new security facilities.

57. HSMM-MESH systems can also make use of *Part 15 on-ramps*, short range systems that provide 802.11i security and gateway to an Amateur Radio network. Through the use of these on-ramps, they can provide wireless access to their networks from systems that can not be modified as Linux can, including Microsoft Windows and Apple iOS.

## Conclusion

58. I recommend that the petition be dismissed without prejudice. This issue could be taken up again if there is ever a real need, and then only after the Amateur community has fully debated the issue and produced a plan which it can request of FCC in detail.

## In Closing

I respectfully submit this comment for the commission's consideration.

*Bruce Perens*

Contact Information:

bruce@perens.com

510-4PERENS (510-4-73-73-67)

Bruce Perens
PMB 549
1563 Solano Ave.
Berkeley CA 94707
USA